NASA Policy Directive

NPD 2800.1E
Effective Date: December 09, 2019
Expiration Date: December 09, 2024

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Managing Information Technology

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. It is NASA policy to ensure that information technology (IT) and information resources are planned, acquired, and managed in a manner that complies with the policies, procedures, and priorities of the Agency and the Federal Government.

b. It is NASA policy to govern NASA's IT direction, mission alignment, investments, and accountability to maximize the value of the Agency's IT contribution to NASA's missions, partners, and the public.

c. It is NASA policy to strategically manage IT activities by ensuring that IT and information resources support achievement of the Agency's goals and objectives. Strategic IT management activities promote the effective, secure, and efficient use of IT throughout the Agency to increase productivity and safety while enabling robust operation, responsiveness, and effectiveness of the Agency's programs.

2. APPLICABILITY

a. This directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers (Agency-wide).

b. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" denotes a discretionary privilege or permission, "can" denotes statements of possibility or capability, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

c. This NASA Policy Directive (NPD) applies to all NASA IT and information resources, including operational technology, as defined by U.S. Federal Code 40 U.S.C. 11101, and mission systems. IT and information resources are defined as any equipment or system that is used in the acquisition, storage, retrieval, manipulation and/or transmission of data or information. Information resources include computers, ancillary and peripheral equipment, software, firmware, and physical devices. This definition applies unless expressly excluded by the NASA Chief Information Officer (CIO).

d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

e. The NASA CIO exercises two types of authorities:

(1) IT Authority, which refers to portfolio investment insight and oversight, enterprise architecture compliance, policy compliance, and cybersecurity compliance for all NASA IT and information resources. IT Authority provides insight and influence on all IT investments in order to mitigate resource risks by using data to drive better purchasing of hardware and software and to enable proper cybersecurity mitigation planning and risk reduction. The NASA CIO may delegate IT Authority to Associate CIOs (ACIOs) and IT Program Executives (PEs).

(2) IT Program Authority, which refers to the management oversight, implementation, and operations of IT services and products. The NASA CIO exercises IT Program Authority for services managed by the NASA CIO. The NASA CIO may delegate IT Program Authority to an Associate CIO or Center CIO.

3. AUTHORITY

a. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 et seq.

b. The Federal Information Technology Acquisition Reform Act (FITARA), 2014, 40 U.S.C. § 11319.

c. E-Government Act of 2002 (Public Law 107-347), as amended, 44 U.S.C. 3601 et seq.

d. The National Aeronautics and Space Act, as amended, 51 U.S.C. 20013 (a) & (h).

e. Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283 (2014). f. NPD 1000.3, The NASA Organization.

4. APPLICABLE DOCUMENTS AND FORMS

a. NPD 1001.0, NASA Strategic Plan.

b. NASA Information Technology Strategic Plan.

5. RESPONSIBILITY

a. The NASA CIO shall:

(1) Advise and assist the Administrator and other Agency senior staff, and participate on the Agency Strategic Management Council, Mission Support Council, and Agency Program Management Council.

(2) Ensure that IT and information resources are strategically managed in a manner that enables achievement of NASA's goals and objectives, and complies with Federal policies and guidance.

(3) Partner with the Chief Financial Officer (CFO) to be responsible and accountable for Agency IT investments and to jointly define the level of detail at which IT resources levels are described.

(4) Advise the Administrator whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component.

(5) Select and manage a member of the CEC to represent Agency IT matters.

(6) Select and manage Center CIOs.

(7) Designate the Senior Agency Information Security Officer (SAISO).

(8) Designate a Senior Agency Official for Privacy (SAOP). .

(9) Designate the Agency Chief Data Office (CDO).

(10) Delegate the role of Authorizing Official for select NASA mission systems Programs and Projects, as appropriate.

(11) Partner with Mission Directorates and the Mission Support Directorate on IT matters.

(12) Conduct IT governing activities. Under the NASA CIO's delegated authority from the Information Technology Council (ITC), charter boards to facilitate IT governing activities such as evaluation of the Agency's business conditions and needs, setting strategy and direction, and overseeing performance outcomes. Establish, maintain, and communicate Agency-wide IT governing structure.

(13) Conduct IT management activities. Establish, articulate, and adjust NASA's IT vision, strategy, outcomes, priorities, and metrics in coordination with Mission Directorates, the Mission Support Directorate, and Centers. Align resources and oversee implementation of supporting IT policies, programs, and activities. Represent the Agency in Federal activities involving IT or information management and ensure the successful completion of related E-Government actions. Monitor and assess IT-related performance to enable achievement of the goals and outcomes in the NPD 1001.0 and the NASA IT Strategic Plan. Communicate information concerning NASA's IT activities.

(14) Conduct IT policy and compliance management. Develop, implement, and enforce Agency policies, procedures,

standards, and guidelines related to IT and information resources, in alignment with Federal policies and guidance.

(15) Conduct risk management. Integrate risk management into the Agency's IT processes to identify, assess, prioritize, and manage risks related to achieving NASA's IT goals and objectives. Safeguard NASA's data and IT assets through an Agency-wide cybersecurity capability that enables cybersecurity mitigation planning and risk reduction.

(16) Oversee NASA's enterprise architecture (EA). Develop, implement, and maintain NASA's IT EA in alignment with Federal and NASA policies and guidance.

(17) Conduct IT workforce planning. Ensure the competency and motivation of NASA's IT workforce through effective recruiting, hiring, training, mentoring, professional development, and incentives to support achievement of NASA's missions, goals, and objectives.

(18) Conduct IT-related innovation. Identify, test, and implement emerging IT and processes in support of NASA's changing technology and business needs. Engage stakeholders in data management, data standards, interoperability, open innovation, and technology infusion in alignment with Agency priorities.

(19) Oversee and optimize NASA's IT portfolio and resources. Lead NASA's IT budget formulation, portfolio management, and investment oversight. Ensure that IT investments align with the goals and outcomes in the NASA Strategic Plan and the NASA IT Strategic Plan, and allocate resources in support of IT programs and projects. Select, control, and evaluate IT investments using the Capital Planning and Investment Control (CPIC) process in alignment with NASA's Planning, Programming, Budgeting, and Execution (PPBE) process. Analyze and optimize the Agency's IT investment portfolio across NASA's IT programs, Centers, and Mission Directorates. Approve NASA's IT budget request. Develop IT operating and execution plans, execute the budget during the performance cycle, and perform budgetary oversight across the IT portfolio. Certify that IT resources are adequately implementing incremental development.

(20) Perform IT contract management for NASA IT investments and contracts that include IT. Manage the life cycle of current and planned IT contracts, including delivery of IT products and services by third party vendors and external service providers. Oversee contract performance.

(21) Conduct IT program management for NASA IT investments and contracts that include IT. Manage IT programs as integrated end-to-end services that increase cybersecurity, efficiency, and inter-Center collaboration. Establish and support a structured approach to manage IT programs. Conduct regular reviews of program and project performance, evaluating the current and projected status toward established requirements, objectives, and performance goals.

(22) Perform IT reporting. Oversee IT reporting as required by Congress, the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and other external entities.

(23) Perform continuous improvement. Benchmark Agency processes against the private and public sectors to promote continuous improvement of IT services and management.

b. Associate CIOs and the Senior Advisor for Cybersecurity shall:

(1) Operate as an extension of the NASA CIO and shape the strategic direction and evolution of IT services.

(2) Share accountability with the NASA CIO for effective oversight and management of IT assets and services.

(3) Select and manage IT Program Executives, where appropriate, with the concurrence of the NASA CIO.

(4) Provide oversight of the planning, design, integration, and delivery of NASA's IT projects and services. Exercise IT authority, including investment review, architecture compliance, and cybersecurity compliance for all IT to mitigate resource risks.

(5) Be responsible for cybersecurity risk mitigation planning, compliance, and risk reduction.

c. Senior Agency Information Security Officer (SAISO) shall:

(1) Carry out the CIO's responsibilities for ensuring Agency compliance with the law, including development, documentation, and implementation of the Agency-wide information security program. SAISO role and cybersecurity program details are documented in NPR-2810.

d. Senior Advisor for Cybersecurity shall:

(1) Operate as an extension of the NASA CIO and shape the strategic direction and evolution of IT services.

(2) Share accountability with the NASA CIO for effective oversight and management of IT assets and services.

(3) Select and manage IT Program Executives, where appropriate, with the concurrence of the NASA CIO.

e. IT Program Executives shall:

(1) Be responsible for the strategy, plans, design, implementation, and delivery of IT services for an assigned IT program, in alignment with the goals and outcomes in the NASA Strategic Plan and the NASA IT Strategic Plan. Develop and maintain roadmaps for their assigned IT program.

(2) Provide oversight and stewardship of resources for an assigned IT program and oversee performance and risk management for the IT program.

(3) Exercise delegated IT authority for all IT within the assigned IT program. Maintain the architecture for the assigned IT program and ensure integration with other IT programs.

(4) Ensure IT program capabilities and projects are initiated and executed throughout their life cycle according to policy and in accordance with approved processes.

f. Each Center Director and Mission Directorate Associate Administrator, with the NASA CIO's concurrence, shall:

(1) Communicate with Center CIOs and Mission Directorate IT Representatives to identify gaps in IT services and elevate issues that are critical to the respective Centers and Mission Directorates.

(2) Provide visibility into Center and Mission Directorate IT investments to enable mitigation of Agency-wide IT resource and cybersecurity risks.

(3) Implement risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. Ensure that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

(4) Ensure that their programs and projects implement cybersecurity requirements established in NPR 2810.1, Security of Information Technology.

g. Center CIOs shall:

(1) Operate as an extension of the NASA CIO and help shape strategic direction and evolution of IT services.

(2) Share accountability with the NASA CIO for effective implementation, operations, utilization, and evaluation of IT services.

(3) Exercise delegated IT authority for all IT within the Center, in partnership with the IT Program Executives.

(4) Act as a representative on IT matters at their Centers.

(5) Implement a Center IT governance process that is supportive of, aligned with, and integrates with the Agency IT governance process. Participate in other Center governance processes where IT is included.

(6) Collaborate with stakeholders to identify requirements to improve IT services.

(7) Provide the NASA CIO with visibility into and awareness of Center IT.

h. Mission Directorates shall:

(1) Identify an Agency-level IT Representative to ensure mission entities and IT matters are represented in the development of policies and procedures, especially those pertaining to cybersecurity.

(2) Enable mitigation of Agency-wide IT resource and cybersecurity risks.

(3) Ensure mission programs and organizations participate and comply with IT policy and governance processes.

(4) Participate in governance boards.

6. DELEGATION OF AUTHORITY

The NASA CIO delegates to Associate CIOs, Center CIOs, and IT Program Executives IT Authority and IT Program Authority, as well as the accountability and responsibility to ensure that NASA IT strategies, policies, architectures, investments, support services, procedures, standards, guidelines, and practices align with Federal and Agency requirements and directions. Center CIOs, Associate CIOs, and IT Program Executives shall support the NASA CIO in the discovery and analysis of IT investments and ensure compliance of IT investments with the Agency's policies

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

and procedures.

7. MEASUREMENT/VERIFICATION

Outcomes and performance measures related to the implementation of this policy are outlined in documents such as NPD 1001.0 and the NASA IT Strategic Plan, as well as in IT-related metrics in NASA's Annual Performance Plan and Federal cross-agency initiatives. Verification occurs through the NASA CIO's performance monitoring and the Agency's Baseline Performance Review (BPR). Results are reported through NASA's annual strategic review, NASA's annual Volume of Integrated Performance, the Agency's annual statement of assurance process, FISMA reporting, and reporting as directed by OMB.

8. CANCELLATION

NPD 2800.1A, Managing Information Technology, March 21, 2008.

/s/Jim Bridenstein
Administrator

ATTACHMENT A: (TEXT)

ATTACHMENT A: Definitions

Operational Technology (OT) - Hardware and software that is physically part of, dedicated to, or essential in real time to the performance, monitoring, or control of physical devices and processes.

ATTACHMENT B: Acronyms

ACIO - Associate Chief Information Officer

BPR - Baseline Performance Review

CEC - CIO Executive Council

CFO - Chief Financial Officer

CIO - Chief Information Officer

CPIC - Capital Planning and Investment Control

EA - Enterprise Architecture

FISMA - Federal Information Security Modernization Act

FITARA - Federal Information Technology Acquisition Reform Act

GAO - Government Accountability Office

IT - Information Technology

ITC - Information Technology Council

NASA - National Aeronautics and Space Administration

NPD - NASA Policy Directive

NPR - NASA Procedural Requirements

OMB - Office of Management and Budget

PE - Program Executive

PPBE - Planning, Programming, Budgeting and Execution

US - United States

U.S.C. - United States Code

ATTACHMENT C: References

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

C.1 The Rehabilitation Act, 29 U.S.C 794d, Sec. 508.

C.2 Preparation, Submission, and Execution of the Budget, OMB Circular A-11.

C.3 Management of Federal Information Resources, OMB Circular A-130.

C.4 NPD 1000.0, NASA Governance and Strategic Management Handbook.

C.5 NPD 1000.3, The NASA Organization.

C.6 NPD 1440.6, NASA Records Management.

C.7 NPD 1490.1, NASA Printing, Duplicating, and Copying Management.

C.8 NPD 2081.1, Nondiscrimination in Federally Assisted and Conducted Programs of NASA.

C.9 NPD 2200.1, Management of NASA Scientific and Technical Information (STI).

C.10 NPD 2810.1, NASA Information Security Policy.

C.11 NPD 2830.1, NASA Enterprise Architecture.

C.12 NPD 7120.4, NASA Engineering and Program/Project Management Policy.

C.13 NPR 1382.1, NASA Privacy Procedural Requirement.

C.14 NPR 2800.1, Managing Information Technology.

C.15 NPR 2810.1, Security of Information Technology.

C.16 NPR 2830.1, NASA Enterprise Architecture Procedures.

C.17 NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

C.18 NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

C.19 NPR 7150.2, NASA Software Engineering Requirements.

C.20 NASA IT Strategic Plan.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.